SOC IMS: SWI-20111206-233204

Last Updated: 1/9/2013 5:20 PM

SOC Incident Management System

IMS User Contact:	(b) (7)	**Restrict Access To:**	All IMS
Record Permissions Group:	All IMS Users	**Record Source:**	

Contact Details

Enter the NASA AUID or email address of the Contact, and click "Lookup Contact Details" to automatically retrieve the information.

AUID:		**Email:**	

Enter Contact information below if the primary contact is not an IMS user

Contact Last Name:	(b) (7)	**Contact First Name:**	(b) (7)
Contact Role:	NASA Other	**Contact Office Phone:**	
Contact E-mail:	(b) (7)(C), (b) (6)	**Contact Cell Phone:**	
Contact AUID:		**Contact NASA Center:**	
Contact Building:		**Contact Room Number:**	
Contact Type:			

General Details

SOC Tracking Number:	SWI-20111206-233204	**Categorization:**	Work-Item
Date Record Created (UTC):	12/6/2011 6:51 PM	**Incident Time Zone:**	UTC - Coordinated Universal Time Zone (GMT)
Title:	Pastebin data		

Brief Description:	Please forward this to tier 2...I remember the (b) (6), (b) name coming up before, but this was posted on PasteBin (HZCj4LXb) on august 13, 2011. ----- Nasa Vulnerable to a public SQLi Exploit - Embarassing much? Admin Username: (b) Email: (b) (6), (b) (7)(C) v Hashed Password: (b) (7)(E) Admin Username: (b) (6), Email (b) (6), (b) (7)(C) Hashed Password: (b) (7)(E) (b) (7)(E) If shit like this is vulnerable to public exploits, imagine whats vulnerable to private 0days :) - [+] TriCk - TeaMp0isoN [+] Shoutouts: iN^SaNe - Hex00010 - MLT Twitter: @TeaMp0isoN_ **NOTE: A joint #TeaMp0isoN & #Anonymous Operation is about to hit the interwebs soon ** ----- Thanks, (b) (6), (b) Special Agent NASA Office of Inspector General, Computer Crimes Division (b) (7)(C), (b) (6) (O) (b) (6), (b) (C) (b) (6), (b) (b) (6), (b) (7)(C) ! WARNING ! This email including any attachments is intended only for authorized recipients. Recipients may only forward this information as authorized. This email may contain non-public information that is "Law Enforcement Sensitive," "Sensitive but Unclassified," or otherwise subject to the Privacy Act and/or legal and other applicable privileges that restrict release without appropriate legal authority and clearance. Accordingly, the use, dissemination, distribution or reproduction of this information to or by unauthorized or unintended recipients, including but not limited to non-NASA recipients, may be unlawful.

Current Status:	Closed	**Assigned To:**	SOC Tier-2
Current Priority:	Low	**Also Notify:**	
CUI:	No SBU or PII	**Notify on Save:**	No
Ok To Close:	Yes		

Work Item Due Date

Due Date:		**Due Date (UTC):**	

Related Tasks

Task ID	Assigned To	Due Date (UTC)	Priority	Status	Description	Resolution
No Records Found						

Related Incidents

Select Relationship:		**Relationship Description:**	

Parent Incident

SOC Tracking Number	Current Status	Title
No Records Found		

Child Incidents

SOC Tracking Number	Current Status	Title
No Records Found		

Sibling Incidents

SOC Tracking Number	Current Status	Title
No Records Found		

Lost or Stolen NASA Equipment Application

Tracking ID	Cause of Loss	Type of System Lost	Description of Circumstances
No Records Found			

Host Information

NASA Hosts

IP Address	IPv6 Address	Host Name	Center/Facility
No Records Found			

External Hosts

IP Address	External IPv6 Address	Host Name	Position in this attack
No Records Found			

Campaigns

Campaign Name:	Hacktivist - Team Poison	**Reviewed By TVA:**	
Campaign Comment:		**Confirmed By TVA:**	(b) (7)(E)

Indicators of Compromise

IOC Domain

FQDN	Do Sinkhole	Comment
No Records Found		

IOC IP

IP Address	IP Block	Comment
No Records Found		

IOC File

Filename	MD5 Hash	Comment
No Records Found		

IOC Registry Key

Key Name	Key Value	Comment
No Records Found		

IOC Email

Sender Email	Subject	Comment
No Records Found		

IOC Detection

Name	Type	Comment

No Records Found

Costs

Center (Hours):		**Center (Dollars):**	
NASA SOC (Hours):	0.50	**NASA SOC (Dollars):**	50.00
NASA NOC (Hours):		**NASA NOC (Dollars):**	
Other Costs (Hours):		**Other Costs (Dollars):**	

Total Costs in Hours and Dollars are automatically calculated as the sum of the individual costs above. Center IR teams or managers should enter the Center costs, the NASA SOC Manager should enter the SOC Costs and the NOC Manager should enter the NOC costs, if any, in order to arrive at the Total Cost.

Total Cost (Hours):	0.5	**Total Cost (Dollars):**	50
Description of Costs:			
System Down Time (Days):		**System Down Time (Hours):**	

Timeline

Date Record Opened (UTC):	12/6/2011 6:51 PM	**Date Record Confirmed (UTC):**	3/13/2012 7:32 AM
Date Record Contained (UTC):	12/6/2011 9:54 PM	**Date Record Resolved (UTC):**	12/6/2011 9:54 PM
Date Record Closed (UTC):	3/13/2012 7:32 AM		
Time in Open:	97.50		
Time in Confirmed:	0.00	**Time to Confirm:**	97.00
Time in Contained:	97.40	**Time to Contain:**	0.13
Time in Resolved:	97.401389	**Time to Resolve:**	0.13
Time in Closed:	2449.99	**Time to Close:**	97.53
Number of Days to Resolve:	0.127		

Journal Entries

Entry	Entry Date	IMS User
Issue already addressed in various other tickets. i.e. SOC Ticket: SOC-20110808-224190 Date: 08/08/2011 IP: (b) (7)(E) Hostname: (b) (6), (b) User: (b) (6), (b) Administrator: (b) (6), (b) Sponsor: PEROT SYSTEMS Code: PX Network: Public (b) (7)(E) Mitigation: (b) (7)(E) Information: Review of the system image found no signs of system level access. A interview with the maintainer confirmed site contained no PII/SBU and was in the process of development before priorities were sidetracked leaving the site below current revision level for a small amount of time. It is unclear when the SQLi/credentials were compromised, but lack of source from the available logs suggest post 3 months. The previous site will be dropped and a new VM/webapp install will be vetted from scratch. Confirmed exposed credentials were only used on the vbulletin instance, and will now be considered lost and never reused in any fashion.	12/6/2011 9:54 PM	(b) (6), (b)
Please forward this to tier 2...I remember the (b) (6), (b) name coming up before, but this was posted on PasteBin (HZCj4LXb) on august 13, 2011. --- Nasa Vulnerable to a public SQLi Exploit - Embarassing much? Admin Username: (b) Email (b) (6), (b) (7)(C) Hashed Password (b) (7)(E) (b) (7)(E) Admin Username (b) (6),	12/6/2011 6:51 PM	(b) (6), (b) (7)

Email: (b) (6), (b) (7)(C)

Hashed Password (b) (7)(E)

(b) (7)(E)

- If shit like this is vulnerable to public exploits, imagine whats vulnerable to private 0days :) -

[+] TriCk - TeaMp0isoN

[+] Shoutouts: iN^SaNe - Hex00010 - MLT

Twitter:

@TeaMp0isoN_

**NOTE: A joint #TeaMp0isoN & #Anonymous Operation is about to hit the interwebs soon **

Thanks,

(b) (6), (b)
Special Agent
NASA Office of Inspector General,

Computer Crimes Division

(b) (7)(C), (b) (6)
(O) (b) (6), (b)
(C) (b) (6), (b) (7)(C)

! WARNING ! This email including any attachments is intended only for authorized recipients. Recipients may only forward this information as authorized. This email may contain non-public information that is "Law Enforcement Sensitive," "Sensitive but Unclassified," or otherwise subject to the Privacy Act and/or legal and other applicable privileges

Attachment(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

History Log

View History Log